Data Retention Policy

Version 0.3

Version Control

	Last Amended	Author	Action taken
0.1	15/11/2018	Loren Morrison	Document Created
0.2	01/11/2019	Loren Morrison	No changes
0.3	01/11/2020	Kas Khalil	Further review required during 2021 to account for changes to GDPR owing to Brexit

Contents

Introduction

Preferred Management as an organisation holds a great deal of important information that is crucial to the running of its daily business operations. While many information systems can be recovered after an incident, the business critical data that resides in electronic and hard copy forms must be suitably protected. This involves considerations into the confidentiality, integrity and availability (CIA) of business critical and potentially sensitive data.

The following policy is designed to the ISO 27001 standard, therefore, it shall be reviewed, and updated regularly to ensure that it remains appropriate in the light of any changes to legal, contractual or acceptable use obligations.

Purpose

The purpose of this Data Retention Policy is to provide guidance on the retention of the various types of data Preferred Management] holds. This document strives to balance the need to store information with legal obligations to destroy the data safely when it is no longer required.

It is anticipated that this policy will assist Preferred Management in securing compliance with legal and regulatory requirements, including Data Protection Act 1998, EU Global Data Protection Regulation 2018 (GDPR), and the Regulation of Investigatory Powers Act 2016.

As appropriate and effective protection is required for all types of data Preferred Management holds to ensure business continuity and avoid breaches of the law and statutory, regulatory or contractual obligations, the following policy will apply to two key types of data that Preferred Management holds: The company's data, and the customer's data (records).

This Data Retention Policy applies to information in all its various forms. It may be on paper, stored electronically or held on film, or other media. It includes text, pictures, audio and video. It covers information transmitted by post, by electronic means, and by oral communication, including telephone and voicemail. It applies throughout the lifecycle of the information from creation through storage and utilisation to disposal.

Policy Objective

Preferred Management Solutions has over-arching information security and data protection objectives in place, however this policy is in place in order to achieve the following objectives;

- Ensure that information is only held for only as long as necessary, giving due regard to the legal, regulatory, business and individual needs;
- Ensure records are stored in a manner which is appropriate to their purpose; and
- Ensure time-periods for retention, are discussed, agreed and documented.

Data Protection

Preferred Management members of staff will collect, store, process, transmit, and retain personal data under the terms of the Data Protection Act (DPA 1998)/ and The EU Global Data Protection Regulations (GDPR 2018)

The current Data Protection Principles governing the protection of personal data, defines 'Personal data' as any information about an individual from whom you are collecting, the compromise, loss or theft of which could cause distress or harm to that individual.

There are six principles in the new GDPR, which are;

Lawfulness, fairness, and transparency
Data will be processed lawfully. It will be fair, and the way information is processed will be transparent

Purpose limitation;
Data will be collected for specific and legitimate purposes, and can't be processed for other reasons which haven't been declared.

Data Minimisation;
Information will be adequate, and relevant. It will be limited to what is necessary in relation to the purpose of the processing.

Accuracy;
Effort must be taken to ensure the accuracy of the information held, and where it is incorrect it will be corrected as quickly as possible.

Storage Limitation;
Information cannot be held for longer than is necessary for the purposes for which it was originally collected.

Integrity and Confidentiality
Information must be processed in a way that ensures the confidentiality and integrity of the information.

Suspension of Document Destruction; Compliance

In the event Preferred Management is served with any subpoena or request for documents or any employee becomes aware of a governmental investigation or audit concerning Preferred Management or the commencement of any litigation against or concerning Preferred Management, such employee shall inform the Data Protection Officer (DPO) and any further disposal of documents shall be suspended until shall time as the DPO, with the advice of counsel, determines otherwise. The DPO shall take such steps as is necessary to promptly inform all staff of any suspension in the further disposal of documents.

Document Retention

Function: Accounting and Financial

Owner:

Record Description	Retention Period	Guidance
Accounting records	7 years	'Ltd' will retain records for 3 years, however 'PLC' will retain the information for 6 years from the year end.
Annual Financial Statements and Audit Reports	Permanent	
Annual Plans and Budgets	2 years	
Budget and periodic internal financial reports	7 years	
Cancelled Checks – special, such as loan repayment	Permanent	
Corporation Tax Records	7 years	7 years from the year end
Contribution Records	Permanent	Charitable donations and gifts
Credit Card Receipts	3 years	
Documents Evidencing Terms of Gifts	Permanent	Charitable donations and gifts
Employee Expense Reports	7 Years	
General Ledger	Permanent	
Grant Records	7 years	Charitable donations and gifts
Interim Financial Statements	7 years	
Investment Records	7 Years	7 years AFTER sale of the investment
PAYE Records	3 years	3 years after the year end
VAT Records	6 years	6 years after the financial year end

Function: Employment

Owner:

Record Description	Retention Period	Guidance
Personnel Records	5 years	5 years after the termination of employment (Including training records, annual assessments, annual leave)
Employee contracts	10 years	10 years after employment ends
Recruitment records (unsuccessful candidates)	3 months	Minimum of 3 months but no longer than 12mths
Retirement and pension records	Permanent	

Function: Health & Safety

Owner:

Record Description	Retention Period	Guidance
Records of reportable injuries, accidents, disease or dangerous events.	3 Years	A minimum of 3 years, or possibly 'Permanent' dependent upon the situation. (RIDDOR)
Accident Book	3 Years	3 years from the date of each entry
List of employees who could be exposed to biological events	40 Years	

Record Description	Retention Period	Guidance
Health records, reports on employees liable to be exposed to hazardous materials	40 Years	
Driver's log book	2 years	
Records of disposal or recovery of hazardous waste	3 Years	

Function: Information Security & Data Protection

Owner:

Record Description	Retention Period	Guidance
Evidence of 'Consent' obtained	Permanent	Whilst marketing continues, evidence should be retained
Records of processing activities	Permanent	As required by the GDPR (Article 32)
Data Protection Impact Assessments	3 Years	3 Years following the end of a project or service
Subject Access Requests (SAR)	3 Years	3 Years following the closure of any such request
Visitor logs	1 Year	Site visit logs
CCTV footage	3 months	Part of a 'cycle' process which will 'overwrite' previous periods recordings.
Results of audits (including technical 'Penetration Tests)	1 Year	

Function: Insurance

Owner:

Record Description	Retention Period	Guidance
Annual Loss Summaries	10 years	
Audits and Adjustments	3 years	3 years after final adjustment
Certificates Issued to [YOUR COMPANY]	Permanent	
Claims Files (including correspondence, medical records, injury documentation, etc.)	Permanent	
Group Insurance Plans - Active Employees		Until Plan is amended or terminated
Group Insurance Plans – Retirees	Permanent	Permanent or until 6 years after death of last eligible participant
Inspections	3 years	
Insurance Policies (including expired policies)	Permanent	
Journal Entry Support Data	7 years	
Loss Runs	10 years	
Releases and Settlements	25 years	

Function: Contracts

Owner:

Record Description	Retention Period	Guidance
Contracts and Related Correspondence (including any proposal that resulted in the contract and all other supportive documentation)	7 years	…after expiration or termination
Licenses and Permits	Permanent	

General Guidance; Internal correspondence

Most correspondence and internal memoranda should be retained for the same period as the document they pertain to or support. For instance, a letter pertaining to a particular contract would be retained as long as the contract (7 years after expiration). It is recommended that records that support a particular project be kept with the project and take on the retention time of that particular project file.

Correspondence or memoranda that do not pertain to documents having a prescribed retention period should generally be discarded sooner. These may be divided into two general categories:

1. Those pertaining to routine matters and having no significant, lasting consequences should be discarded within two years. Some examples include
   1.1. Routine letters and notes that require no acknowledgment or follow-up, such as notes of appreciation, congratulations, letters of transmittal, and plans for meetings.
   1.2. Form letters that require no follow-up.
   1.3. Letters of general inquiry and replies that complete a cycle of correspondence.
   1.4. Letters or complaints requesting specific action that have no further value after changes are made or action taken (such as name or address change).
   1.5. Other letters of inconsequential subject matter or that definitely close correspondence to which no further reference will be necessary.
   1.6. Chronological correspondence files.

Please note that copies of interoffice correspondence and documents where a copy will be in the originating department file should be read and destroyed, unless that information provides reference to or direction to other documents and must be kept for project traceability.

2. Those pertaining to non-routine matters or having significant lasting consequences should generally be retained permanently.

General Guidance – E-Mail

Not all email needs to be retained, depending on the subject matter. However users should consider carefully the use (and retention) of e-mail, from internal or external sources, and where appropriate, these should be deleted after 12 months.

This Policy

This document is subject to ongoing review as part of the annual review cycle and is signed off, annually by the Head of Operations / Operations Director of Preferred Management who is ultimately accountable for Information Security at Preferred Management